CLAIMS

1. Method for sending messages over secure communication links in networks comprising at least a first terminal being able to change its method of network access and at least one other terminal with one or more possible intermediate computers between the first terminal and the other terminal performing network address and/or other translations, a secure communication link being established between an initial network address of the first terminal and the address of the other terminal, the link defining at least the addresses of the two terminals, and performing encapsulation in said secure communication link to overcome network address and/or other translations made by said intermediate computers on the route, characterized by

   a) the first terminal moving from said initial network address to a new network address,

   b) sending a request message using encapsulation from the first terminal to the other terminal to change said secure connection to be between the new address of the first terminal and the other terminal, the request also containing a description of the encapsulation method performed by the first terminal on the basis of which description the other terminal detects translations performed by said intermediate computers,

   c) the other terminal responding to the first terminal with a reply message with a description about translations made by said possible intermediate computers between the new address of the first terminal and the other terminal and/or encapsulation methods supported by the other terminal, and

   d) thereafter sending the message from the first terminal to the other terminal by using the information sent with said reply.

2. Method of claim 1, characterized in that, the description of the message include source and/or destination addresses on the basis of which the receiving terminal detects address translations performed by intermediate computers.

3. Method of claim 1, characterized in that the description of the message includes information about encapsulation protocols, as well as source and destination TCP or UDP ports.

4. Method of claim 3, characterized in that the NAT traversal is performed by UDP encapsulation, TCP encapsulation and/or by some other encapsulation.

5. Method of any of claims 1 - 4, characterized in that after receiving of the request message by said other terminal sent in step c), the other terminal determines by examining the request, which translations and/or encapsulations are required in the traffic between the first terminal and the other terminal.

6. Method of claim 5, characterized in that the reply message of step c) contains information about the communication link to be used between the new address of the first terminal and said other terminal.

7. Method of claim 6, characterized in that the information about the communication link includes information about whether NAT traversal and/or other encapsulation should be used.

8. Method of any of claims 1 - 5, characterized in that in step c) the first terminal compares the descriptions of the request respective reply messages and sends all subsequent messages from this new network address on the basis of the comparison telling what encapsulations, protocols and rules should be used in the further communication.

9. Method of any of claims 1 - 8, characterized in that the secure communication link is formed by using the IPSec protocol.

10. Method of claim 9, characterized in that the message in step d) is sent by using IPSec and NAT traversal updated to the new network address of the first terminal.

11. Method of claim 7 or 8, characterized in that the message in step d) is sent without NAT traversal in the communication link if on the basis of the comparison in claim 8, the descriptions correspond to each other or if so informed by the other terminal in claim 7.

12. Method of any of claims 1 -11, characterized in that the secure connection is an IPSec SA.

13. Method of claim 12, characterized in that for forming the IPSec SA, a key exchange mechanism that passes through NAT is used.

14. Method of claim 12, characterized in that the key exchange protocol is IKE if the NAT device supports the UDP protocol.

15. Method of claim 14, characterized in that for forming the IPSec SA, a key exchange mechanism is used wherein several traversal mechanisms are used simultaneously to increase the chance that at least one of them pass through the NAT device.

16. Method of claim 12, characterized in that for forming the IPSec SA, a key exchange mechanism is performed in which a negotiation process is used to agree on protocols to be used in the further communication.

17. Method of claim 12, characterized in that for forming the IPSec SA, an encapsulation protocol is used in the key exchange mechanism.

18. Method of any of claims 1 - 17, characterized in that the address of the other terminal is the end destination address of messages sent from the first

terminal, in which case transport or tunnel mode is used in the IPSec communication.

19. Method of any of claims 1 - 17, characterized in that the destination address of the message is the address of a host which is not the other terminal, in which case tunnel mode or transport mode together with a tunnelling protocol is used in the IPSec communication.

20. Method of any of claims 1 - 7, 9 - 19, characterized in that several request messages of step b) are sent, each processed using a different traversal mechanism, where after the other terminal indicates in the reply which mechanisms to be used in the further communication.